**IN THE CLAIMS:**

The text of all pending claims, (including withdrawn claims) is set forth below. Cancelled and not entered claims are indicated with claim number and status only. The claims as listed below show added text with underlining and deleted text with ~~strikethrough~~. The status of each claim is indicated with one of (original), (currently amended), (cancelled), (withdrawn), (new), (previously presented), or (not entered).

Please CANCEL claim 2 without prejudice or disclaimer.

Please AMEND claims 1, 3, 15, 17, 19, and 30-32 in accordance with the following:

1. (CURRENTLY AMENDED) A data management system comprising:

a storage medium for storing contents;

application executing means for activating an application so that the application accesses the contents stored in the storage medium and effects a processing on the contents;

access monitoring means for monitoring the status of access of the application to the contents by associating inherent information for the application brought into an activated status by the application executing means, with inherent information for the contents accessed by the application; ~~and~~

filtering means for enciphering the contents with the inherent information for the application when the application under the activated status writes the contents into the storage medium while deciphering the contents with the inherent information for the application when the application under the activated status reads out the contents in the storage medium; and

an operating system as a software for controlling the execution of the application, wherein

the operating system assigns identification information to each process upon executing the application by the application executing means, and the access monitoring means utilizes the identification information as the inherent information for the application.

2. (CANCELLED)

3. (CURRENTLY AMENDED) A data management system according to Claim ~~2~~ 1, wherein

the access monitoring means registers the inherent information for the application and the inherent information for the contents in a management table so that the inherent information for the application and the inherent information for the contents are associated with each other,

and the access monitoring means monitors the status of access with the assistance of the management table.

4. (ORIGINAL) A data management system according to Claim 3, wherein

when the application executing means completes the execution of the application, the access monitoring means deletes the inherent information for the application and the inherent information for the contents corresponding to the application from the management table.

5. (ORIGINAL) A data management system according to Claim 3, wherein

at least one piece of logical drive is built in the storage medium and the contents is reserved in the logical drive,

a file system for managing the logical drive is built in each of the logical drive, and

at least one file system is arranged to serve as an encryption file system which has a cryptographic attribute determined for each file or folder containing the contents, enciphers the contents at each file or folder upon storing the contents in the storage medium.

6. (WITHDRAWN) A data management system according to Claim 3, wherein

at least one piece of logical drive is built in the storage medium and the contents is reserved in the logical drive,

a file system for managing the logical drive is built in each of the logical drive, and

at least one file system is arranged to serve as an encryption file system which enciphers the file system as a whole upon storing the contents in the storage medium.

7. (PREVIOUSLY PRESENTED) A data management system according to Claim 5, wherein

when the application reads out the contents stored in the logical drive managed by the encryption file system, the access monitoring means registers a file name of the file containing the contents read out by the application in the management table as the inherent information for the contents.

8. (WITHDRAWN) A data management system according to Claim 6, wherein

when the application reads out the contents stored in the logical drive managed by the encryption file system, the access monitoring means registers a file name of the file containing the contents read out by the application in the management table as the inherent information for

the contents.

9. (ORIGINAL) A data management system according to Claim 5, wherein when the application reads the contents stored in the logical drive managed by the encryption file system, the access monitoring means registers a drive name of the logical drive containing the contents read out by the application in the management table as the inherent information for the contents.

10. (WITHDRAWN) A data management system according to Claim 6, wherein when the application reads the contents stored in the logical drive managed by the encryption file system, the access monitoring means registers a drive name of the logical drive containing the contents read out by the application in the management table as the inherent information for the contents.

11. (ORIGINAL) A data management system according to Claim 5, wherein when the application effects a processing on the contents to create a new file, the access monitoring means registers a file name generated for the new file in the management table so that the file name and the inherent information for the application are associated with each other.

12. (WITHDRAWN) A data management system according to Claim 6, wherein when the application effects a processing on the contents to create a new file, the access monitoring means registers a file name generated for the new file in the management table so that the file name and the inherent information for the application are associated with each other.

13. (ORIGINAL) A data management system according to Claim 11, wherein the access monitoring means changes the file name of the new file partly or wholly, and registers the changed name in the management table.

14. (WITHDRAWN) A data management system according to Claim 12, wherein the access monitoring means changes the file name of the new file partly or wholly, and registers the changed name in the management table.

15. (CURRENTLY AMENDED) A data management system ~~according to Claim 9~~, comprising:

a storage medium for storing contents;

application executing means for activating an application so that the application accesses the contents stored in the storage medium and effects a processing on the contents;

access monitoring means for monitoring the status of access of the application to the contents by associating inherent information for the application brought into an activated status by the application executing means, with inherent information for the contents accessed by the application;

filtering means for enciphering the contents with the inherent information for the application when the application under the activated status writes the contents into the storage medium while deciphering the contents with the inherent information for the application when the application under the activated status reads out the contents in the storage medium; and

an operating system as a software for controlling the execution of the application, wherein the operating system assigns identification information to each process upon executing the application by the application executing means, and the access monitoring means utilizes the identification information as the inherent information for the application, and

wherein

the access monitoring means registers the inherent information for the application and the inherent information for the contents in a management table so that the inherent information for the application and the inherent information for the contents are associated with each other, and the access monitoring means monitors the status of access with the assistance of the management table, and

wherein

at least one piece of logical drive is built in the storage medium and the contents is reserved in the logical drive,

a file system for managing the logical drive is built in each of the logical drive, and

at least one file system is arranged to serve as an encryption file system which has a cryptographic attribute determined for each file or folder containing the contents, enciphers the contents at each file or folder upon storing the contents in the storage medium, and

wherein

when the application reads the contents stored in the logical drive managed by the encryption file system, the access monitoring means registers a drive name of the logical drive containing the contents read out by the application in the management table as the

inherent information for the contents, and

wherein

the access monitoring means compares a drive name of the logical drive as a destination for storing a file, which is newly created when the application effects a processing on the contents, with a drive name of the logical drive registered in the management table, and if it is determined that both of the drive names disagree with each other as the result of comparison, the access monitoring means changes a file name of the newly created file so that the newly created file is stored in the logical drive of the drive name registered in the management table and registers the changed file name in the management table.

16. (WITHDRAWN) A data management system according to Claim 10, wherein the access monitoring means compares a drive name of the logical drive as a destination for storing a file, which is newly created when the application effects a processing on the contents, with a drive name of the logical drive registered in the management table, and if it is determined that both of the drive names disagree with each other as the result of comparison, the access monitoring means changes a file name of the newly created file so that the newly created file is stored in the logical drive of the drive name registered in the management table and registers the changed file name in the management table.

17. (CURRENTLY AMENDED) A data management system ~~according to Claim 9~~, comprising:

a storage medium for storing contents;

application executing means for activating an application so that the application accesses the contents stored in the storage medium and effects a processing on the contents;

access monitoring means for monitoring the status of access of the application to the contents by associating inherent information for the application brought into an activated status by the application executing means, with inherent information for the contents accessed by the application;

filtering means for enciphering the contents with the inherent information for the application when the application under the activated status writes the contents into the storage medium while deciphering the contents with the inherent information for the application when the application under the activated status reads out the contents in the storage medium; and

an operating system as a software for controlling the execution of the application, wherein the operating system assigns identification information to each process upon executing

the application by the application executing means, and the access monitoring means utilizes the identification information as the inherent information for the application, and

wherein

the access monitoring means registers the inherent information for the application and the inherent information for the contents in a management table so that the inherent information for the application and the inherent information for the contents are associated with each other, and the access monitoring means monitors the status of access with the assistance of the management table, and

wherein

at least one piece of logical drive is built in the storage medium and the contents is reserved in the logical drive,

a file system for managing the logical drive is built in each of the logical drive, and

at least one file system is arranged to serve as an encryption file system which has a cryptographic attribute determined for each file or folder containing the contents, enciphers the contents at each file or folder upon storing the contents in the storage medium, and

wherein

when the application reads the contents stored in the logical drive managed by the encryption file system, the access monitoring means registers a drive name of the logical drive containing the contents read out by the application in the management table as the inherent information for the contents, and

the access monitoring means compares a drive name of the logical drive as a destination for storing a file, which is newly created when the application effects a processing on the contents, with a drive name of the logical drive registered in the management table, and if it is determined that both of the drive names are coincident with each other as the result of comparison, then the access monitoring means prohibits a file name of the newly created file from being registered in the management table.

18. (WITHDRAWN) A data management system according to Claim 10, wherein

the access monitoring means compares a drive name of the logical drive as a destination for storing a file, which is newly created when the application effects a processing on the contents with a drive name of the logical drive registered in the management table, and if it is determined that both of the drive names are coincident with each other as the result of comparison, then the access monitoring means prohibits a file name of the newly created file from being registered in the management table.

19. (CURRENTLY AMENDED) A data management system ~~according to Claim 9~~, comprising:

a storage medium for storing contents;

application executing means for activating an application so that the application accesses the contents stored in the storage medium and effects a processing on the contents;

access monitoring means for monitoring the status of access of the application to the contents by associating inherent information for the application brought into an activated status by the application executing means, with inherent information for the contents accessed by the application;

filtering means for enciphering the contents with the inherent information for the application when the application under the activated status writes the contents into the storage medium while deciphering the contents with the inherent information for the application when the application under the activated status reads out the contents in the storage medium; and

an operating system as a software for controlling the execution of the application, wherein the operating system assigns identification information to each process upon executing the application by the application executing means, and the access monitoring means utilizes the identification information as the inherent information for the application, and

wherein

the access monitoring means registers the inherent information for the application and the inherent information for the contents in a management table so that the inherent information for the application and the inherent information for the contents are associated with each other, and the access monitoring means monitors the status of access with the assistance of the management table, and

wherein

at least one piece of logical drive is built in the storage medium and the contents is reserved in the logical drive,

a file system for managing the logical drive is built in each of the logical drive, and

at least one file system is arranged to serve as an encryption file system which has a cryptographic attribute determined for each file or folder containing the contents, enciphers the contents at each file or folder upon storing the contents in the storage medium, and

wherein

when the application reads the contents stored in the logical drive managed by the encryption file system, the access monitoring means registers a drive name of the logical

drive containing the contents read out by the application in the management table as the inherent information for the contents, and

wherein

the access monitoring means compares a drive name of the logical drive as a destination for storing a file, which is newly created when the application effects a processing on the contents with a drive name of the logical drive registered in the management table, and

if it is determined that both of the drive names disagree with each other as the result of comparison, then the operation of the filtering means is validated.

20. (WITHDRAWN) A data management system according to Claim 10, wherein

the access monitoring means compares a drive name of the logical drive as a destination for storing a file, which is newly created when the application effects a processing on the contents, with a drive name of the logical drive registered in the management table, and if it is determined that both of the drive names disagree with each other as the result of comparison, then the operation of the filtering means is validated.

21. (ORIGINAL) A data management system according to Claim 19, wherein

the storage medium comprises a primary storage means which erases data stored therein upon power supply cut, and

the filtering means stores an enciphered version of the newly created file in the primary storage means instead of the logical drive as the storage destination.

22. (WITHDRAWN) A data management system according to Claim 20, wherein

the storage medium comprises a primary storage means which erases data stored therein upon power supply cut, and

the filtering means stores an enciphered version of the newly created file in the primary storage means instead of the logical drive as the storage destination.

23. (ORIGINAL) A data management system according to Claim 5, wherein

the storage medium comprises a first storage unit including the logical drive managed by the encryption file system and a second storage unit for storing therein the contents enciphered by the filtering means.

24. (WITHDRAWN) A data management system according to Claim 6, wherein

the storage medium comprises a first storage unit including the logical drive managed by the encryption file system and a second storage unit for storing therein the contents enciphered by the filtering means.

25. (ORIGINAL) A data management system according to Claim 23, wherein

the application executing means, the access monitoring means, the filtering means and the first storage means are provided within a single unit of data processing apparatus, and

the second storage unit is connected to the data processing apparatus by way of a network.

26. (WITHDRAWN) A data management system according to Claim 24, wherein

the application executing means, the access monitoring means, the filtering means and the first storage means are provided within a single unit of data processing apparatus, and

the second storage unit is connected to the data processing apparatus by way of a network.

27. (WITHDRAWN) A data management system according to Claim 1, further comprising:

authenticating means for carrying out authentication on a user; and

switching means for switching the mode of operation of the filtering means between a valid mode and an invalid mode only when the authenticating means successfully carries out the authentication on the user.

28. (WITHDRAWN) A data management system according to Claim 23, wherein

the application executing means, the access monitoring means, the filtering means and the second storage means are provided within a single unit of data processing apparatus, and

the first storage means is involved in ae data recording reproducing apparatus attached outside the data processing apparatus.

29. (CANCELLED)

30. (CURRENTLY AMENDED) A data processing system comprising:

application executing means for activating an application so that the application accesses the contents stored in a storage medium and effects a processing on the contents;

access monitoring means for monitoring the status of access of the application to the contents by associating inherent information for the application brought into an activated status by the application executing means with inherent information for the contents accessed by the application; and

filtering means for enciphering the contents with the inherent information for the application when the application under the activated status writes the contents into the storage medium while deciphering the contents with the inherent information for the application when the application under the activated status reads out the contents from the storage medium; and

an operating system as a software for controlling the execution of the application, wherein

the operating system assigns identification information to each process upon executing the application by the application executing means, and the access monitoring means utilizes the identification information as the inherent information for the application.

31. (CURRENTLY AMENDED) A recording medium capable of being read by a computer having recorded thereon a data management program which forces the computer to realize a function for protecting a copyright of contents stored in a storage medium when an application accesses the contents to effect a processing on the contents, wherein

the data management program forces the computer to function as access monitoring means and filtering means, the access monitoring means monitoring the status of access of the application to the contents by associating inherent information for the application brought into an activated status with inherent information for the contents accessed by the application and, the filtering means enciphering the contents with the inherent information for the application when the application under the activated status writes the contents into the storage medium while deciphering the contents with the inherent information for the application when the application under the activated status reads out the contents from the storage medium; and

an operating system as a software for controlling the execution of the application, wherein

the operating system assigns identification information to each process upon executing the application by the application executing means, and the access monitoring means utilizes the identification information as the inherent information for the application.

32. (CURRENTLY AMENDED) A data management system comprising:

an access monitor capable of monitoring a status of access of an application to contents

by associating inherent information for the application brought into an activated status with inherent information for the contents accessed by the application; and

a filter capable of enciphering the contents with the inherent information for the application when the application under the activated status writes the contents into a storage medium while deciphering the contents with the inherent information for the application when the application under the activated status reads out the contents in the storage medium; and

an operating system as a software for controlling the execution of the application, wherein

the operating system assigns identification information to each process upon executing the application by the application executing means, and the access monitoring means utilizes the identification information as the inherent information for the application.